КАК СОЗДАТЬ НАДЁЖНЫЙ ПАРОЛЬ

Как показывают исследования, самыми популярными паролями 2021 года у россиян стали «qwerty123», «qwerty1», «123456», «a11111» и «123456789». Среди кириллических паролей — «йцукен», «пароль» и «любовь». Такие пароли легко взломать киберпреступникам — хакеры используют программы и словари с самыми популярными паролями для перебора комбинаций букв, цифр и символов. Рассказываем, как создать надёжный пароль, взлом которого может занять десятки лет

ПРИЗНАКИ НАДЁЖНОГО ПАРОЛЯ

Длинный и его трудно угадать

Надёжный пароль содержит 12 символов, включает буквы в разном регистре, цифры и специальные символы (~!@#$%^&*+-/.,\{}[]();:|?<>=)

В нём нет последовательных комбинаций клавиш

Не используйте последовательный набор клавиш, например, «qwerty», — его легко взломать. Для надёжного пароля применяйте случайную комбинацию букв, цифр и других символов

Нет личных данных

Не используйте для паролей личные данные, например, фамилию, дату рождения или кличку питомца. Такую информацию легко узнать, просмотрев ваши социальные сети

Содержит фразу

Выбирайте за основу не слова, а фразы — они длиннее, их сложнее угадать или перебрать. Используйте для пароля смешное событие, забавную привычку, тайную мечту — такой пароль легко запомнить и трудно подобрать: «ГотовлюБорЩ_на5+баллов!@», «РекордПрохождения$Цивилизации$-32часа», «_Поеду1_вРио-де-Жанейро-вБелыхШт@н@х»

Уникальный

Придумайте пароль для каждого критичного аккаунта — интернет-банка, соцсетей и Госуслуг. Если один и тот же пароль используется в разных сервисах, взломав один, злоумышленники получат доступ ко всем вашим аккаунтам

Для аккаунтов, в которых не хранятся важные данные и не совершаются покупки, можно придумать простой и даже повторяющийся пароль

ИДЕИ ДЛЯ СОЗДАНИЯ НАДЁЖНОГО ПАРОЛЯ

Используйте генераторы паролей — программы, которые формируют случайные комбинации по заданным требованиям

КАК СОХРАНИТЬ ПАРОЛИ В БЕЗОПАСНОСТИ

Не сохраняйте пароли на смартфоне, планшете или компьютере

Если злоумышленники получат доступ к вашему устройству, они легко доберутся до паролей. Также небезопасно хранить пароли в браузерах — в них периодически находят уязвимости, которыми могут воспользоваться хакеры, чтобы добраться до ваших паролей

Используйте двухфакторную аутентификацию (2FA)

Это метод защиты аккаунта не только посредством ввода логина и пароля, но и при помощи кода, известного только вам как владельцу аккаунта. Код может быть отправлен по смс или на электронную почту, а также создан специальным приложением-генератором одноразового кода: Twilio Authy, Duo Mobile и «Яндекс.Ключ»

2FA — дополнительный уровень безопасности, так вы усложните путь хакерам. Плюс 2FA помогает предотвратить взлом. Если вы получили смс с кодом, который не запрашивали, значит, аккаунт пытаются взломать, нужно срочно сменить пароль

На некоторых сайтах. например, в Госуслугах пользователи также могут настроить двухфакторную аутентификацию. Вход с подтверждением по смс нужен для безопасного доступа к личному кабинету и данным на портале. При каждом входе на Госуслуги будет приходить смс с одноразовым кодом подтверждения. Этот код нужно указывать после ввода пароля. Помните, что его никому нельзя сообщать

Используйте менеджер паролей

Это специальные программы, которые генерируют, хранят и управляют вашими паролями в одном безопасном онлайн-аккаунте. Так, вам придётся запомнить только один сложный пароль — мастер-пароль от хранилища, где будут собраны все ваши пароли

Храните пароли в тайне

Не сохраняйте их «на листочке» на видном месте, не отправляйте через текстовое сообщение или электронную почту. Даже если вы доверяете человеку, кто-то другой может завладеть и воспользоваться паролем в корыстных целях

РЕЗЮМЕ

Используйте сложные пароли длиной 12 знаков, которые содержат заглавные и строчные буквы, цифры и специальные символы

Используйте для паролей случайную комбинацию букв, цифр и других

символов. Подойдут забавные фразы, которые нужно записывать буквами разного регистра и добавляя цифры и символы

Не используйте для паролей личные данные или другую информацию, которую публикуете вы или ваши близкие в социальных сетях

Храните пароли в специальных программах — менеджерах паролей

Используйте разные пароли для каждой важной учётной записи

Не храните пароли на бумажных носителях, в электронных блокнотах, заметках и браузерах

Обязательно используйте двухфакторную аутентификацию